UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte HIDEKI KOIKE and TETSUJI TAKADA

Appeal 2007-1815
Application 09/710,203
Technology Center 2100

Decided: October 31, 2007

Before LEE E. BARRETT, ANITA PELLMAN GROSS, and ALLEN R. MACDONALD, *Administrative Patent Judges*.

MACDONALD, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF CASE

Appellants appeal a rejection of claims 1-6, 8-21, and 23-26 under 35 U.S.C. § 134 (2002). We have jurisdiction under 35 U.S.C. § 6(b) (2002).

THE INVENTION

Appellants invented a system and method for maintaining secure log files and more specifically, a system and method for restoring an altered or

deleted log file with an unaltered log file from a plurality of identical log files. (Spec. 3:33 to 4:2.)

Claims 1 and 26 are reproduced below:

1. A log file protection system for protecting log files in which computer system operations have been recorded, comprising:

log file creation means which create a plurality of identical log files which record the operations of said computer system;

alteration detection means which periodically monitor said plurality of identical log files for alteration or deletion; and

restoration means which restore an altered or deleted log file by replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files when the altered or deleted log file is detected by said alteration detection means.

26. A log file protection method for protecting log files in which computer system operations have been recorded, comprising:

(a) creating a plurality of identical log files which record the operations of said computer system;

(b) periodically monitoring said plurality of identical log files for alteration or deletion; and

(c) restoring the altered or deleted log file[1] by replacing the altered or deleted log file with an unaltered log file from the plurality of identical log files when the altered or deleted log file is detected in said periodic monitoring step.

[1] We note the lack of antecedent basis for "the altered or deleted log file."

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Schneier and Kelsey, *Cryptographic Support for Secure Logs on Untrusted Machines*, Core SDI S.A., 53-62 (1998), (hereinafter "Schneier").

Claims 1-6, 8-21, and 23-26[2] stand rejected under 35 U.S.C. § 102(a) as being anticipated by Schneier.

Rather than repeat the arguments of Appellants or the Examiner, we make reference to the Briefs and the Answer for their respective details. Only those arguments actually made by Appellants have been considered in this decision. Arguments which Appellants could have made but chose not to make in the Briefs have not been considered and are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii) (2004).

We reverse.

ISSUE

Have Appellants shown that the Examiner has erred in finding that the claims are anticipated over the disclosure of Schneier under 35 U.S.C. § 102(a)? The issue turns on whether Schneier discloses replacing an altered

[2] We note that the statement of the rejection in the Answer and the entire explanation deals only with independent claims 1 and 26. (Answer 3-5.) We address dependent claims 2-6, 8-21, and 23-25 because Appellant has appealed the rejection of those claims. (Br. 7 and 12.)

or deleted log file with an unaltered log file from a plurality of identical log files.

FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

1. Schneier discloses a scheme for securing log files by transferring a log file from an untrusted machine U to a trusted machine T. (Section 1, ¶ 11, ll. 3-7.)
2. Schneier discloses that a moderately trusted verifier V monitors and verifies parts of a log file. (Section 3.1, ¶ 5, ll. 3-5 and Section 3.5, ll. 1-3.)
3. Schneier discloses replacing data on a machine with data recovered from a clean backup in the event that the machine has been determined to have been attacked based on monitoring of the log file. (Section 5, ¶ 1, ll. 12-22.) Schneier explains:

> The victims could then revoke some public key certificates, inform users that their *data* may have been compromised, wipe the machine's storage devices and restore it from a clean backup, or improve physical and network security on the machine to prevent further attacks. (Emphasis added) (Section 5, ¶ 1, ll. 17-22.)

4. Schneier does not disclose that the recovered data includes a log file.

5. Schneier discloses that the log file that is inspected by verifier V is not alterable by the verifier V. Schneier explains:

> V is now able to decrypt and read, *but not to change*, the log entries whose keys were sent in M_4. (Emphasis added) (Section 3.5, ¶ 9, ll. 1-3.)

6. Accordingly, Schneier does not disclose that an altered or deleted *log file* is replaced with another log file.

PRINCIPLES OF LAW

It is axiomatic that anticipation of a claim under § 102 can be found only if the prior art reference discloses every element of the claim. *See In re King*, 801 F.2d 1324, 1326, 231 USPQ 136, 138 (Fed. Cir. 1986) and *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1458, 221 USPQ 481, 485 (Fed. Cir. 1984).

ANALYSIS

Appellants have not presented any substantive arguments directed to the separate patentability of dependent claims 2-6, 8-21, and 23-25, but rely instead on their arguments for patentability of independent claim 1. In the absence of a separate argument with respect to the dependent claims, those claims stand or fall with the representative independent claims. *See In re Young,* 927 F.2d 588, 590, 18 USPQ2d 1089, 1091 (Fed. Cir. 1991). *See also* 37 C.F.R. § 41.37(c)(1)(vii)(2004).

Here, claims 1-6, 8-21, and 23-26 are subject to the same rejection. Because the Appellants argue only the limitations of claims 1 and 26 (Br. 12-15[3] and Reply Br. 2-6) and because claims 1 and 26 have substantially the same limitations, we select claim 26 as the sole claim on which to decide the appeal of all the claims.

35 U.S.C. § 102(a)

We find that the Examiner erred in rejecting claim 26 under 35 U.S.C. § 102(a) by not showing that Schneier discloses all elements of claim 26.

The Examiner finds instant claim 26 to be anticipated by Schneier, as set forth at page 7 of the Answer. Claim 26 has elements other than element (c), but we focus our analysis on element (c). Element (c) of claim 26 requires that an altered or deleted log file be replaced by another log file. The Examiner finds that Schneier discloses element (c) of claim 26 by two passages: (1) the transmission of A_0, a random starting point in a log file (Schneier, Section 4.2, col. 2) and (2) restoring data to a machine from a clean backup (Schneier, Section 5, ¶ 1). (Answer 7.)

We acknowledge that Appellants have alleged that Schneier does not teach element (b),[4] however, in deciding that the Examiner has erred in

[3] We refer to the Second Appeal Brief filed June 26, 2006.
[4] We suggest that the Examiner consider whether Schneier's moderately trusted verifier V (e.g., Section 2, ¶ 6; Section 3.1, Subsection 5, ll. 2-5; and Section 3.5, ll. 1-3) discloses element (b) of claim 26.

rejecting claim 26 as being anticipated by Schneier, we rely solely on our finding that Schneier does not disclose element (c) of claim 26.[5] Schneier discloses that *data* is restored to a machine having a log file. (FF 3.) But Schneier does not disclose that the restored data includes a *log file*. (FF 4.) Rather, Schneier discloses that the verifier V is not to change log entries, thereby leaving log files unchanged. (FF 5.) We find that Schneier does not disclose that an altered or deleted log file is replaced with another log file. (FF 6.) Accordingly, Schneier does not disclose element (c) of claim 26.

The decision of the Examiner is reversed.

NEW GROUNDS OF REJECTION

35 U.S.C. § 112, second paragraph

Using our authority under 37 C.F.R. § 41.50(b), we reject claim 25 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Appellants regard as the invention. Claim 25 recites:

> 25. Recording media which stores a program capable of implementing the log file protection system according to any of Claims 1-6, 8-21 or 23-24 on a computer system.

The use of the phrase "capable of" renders claim 25 vague and indefinite because it is unclear whether the limitations following the phrase are ever part of the claimed invention.

[5] Claim 1 includes a similar limitation as element (c) of claim 26.

37 C.F.R. § 41.50(b)

37 C.F.R. § 41.50(b) provides that, "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review."

37 C.F.R. § 41.50(b) also provides that the Appellants, *WITHIN TWO MONTHS FROM THE DATE OF THE DECISION*, must exercise one of the following two options with respect to the new grounds of rejection to avoid termination of appeal as to the rejected claims:

> (1) *Reopen prosecution*. Submit an appropriate amendment of the claims so rejected or new evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the proceeding will be remanded to the examiner …
>
> (2) *Request rehearing*. Request that the proceeding be reheard under 37 C.F.R. § 41.52 by the Board upon the same record …

CONCLUSIONS OF LAW

(1) Appellants have shown that the Examiner erred in finding that claims 1-6, 8-21, and 23-26 are anticipated by Schneier under 35 U.S.C. § 102(a).

(2) Claim 25 is unpatentable for failing to comply with 35 U.S.C. § 112, second paragraph.

DECISION

The Examiner's rejection of claims 1-6, 8-21, and 23-26 under 35 U.S.C. § 102(a) is reversed.

Claim 25 is rejected under 35 U.S.C. § 112, second paragraph.

New grounds of rejection have been entered under 37 C.F.R. § 41.50(b).

REVERSED

37 C.F.R. § 41.50(b)

rwk

CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE WA 98101-23